

МІНІСТЕРСТВО ОСВІТИ І НАУКИ, МОЛОДІ ТА СПОРТУ УКРАЇНИ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ «КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ» ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ

Комп'ютерний практикум №2

з дисципліни Криптографія:

«Криптоаналіз шифру Віженера»

Виконали:

Студенти групи ФБ-96 Сендецький Костянтин Твердохлібов Денис

Мета роботи

Засвоєння методів частотного криптоаналізу. Здобуття навичок роботи та аналізу потокових шифрів гамування адитивного типу на прикладі шифру Віженера.

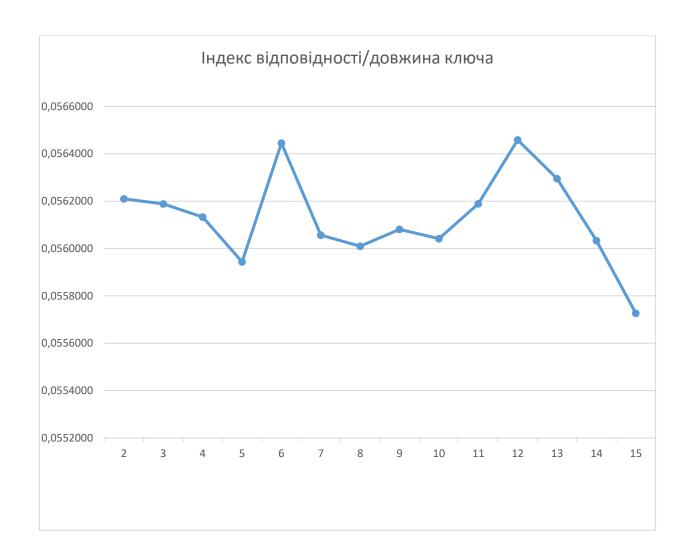
Порядок виконання роботи

- 0. Уважно прочитати методичні вказівки до виконання комп'ютерного практикуму.
- 1. Самостійно підібрати текст для шифрування (2-3 кб) та ключі довжини r = 2, 3, 4, 5, а також довжини 10-20 знаків. Зашифрувати обраний відкритий текст шифром Віженера з цими ключами.
- 2. Підрахувати індекси відповідності для відкритого тексту та всіх одержаних шифртекстів і порівняти їх значення.
- 3. Використовуючи наведені теоретичні відомості, розшифрувати наданий шифртекст (згідно свого номеру варіанта).

Хід роботи

Завдання 1-2. Було взято уривок з «Преступление и наказание». Набір ключів довжиною с 2 до 15. Індекси відповідності для кожного ключа

для кожного клю ш
Індекс відповідності
0.0562101
0.0561887
0.056133
0.0559436
0.0564454
0.0560568
0.0560096
0.0560811
0.0560416
0.0561889
0.0564588
0.0562952
0.0560336
0.0557263

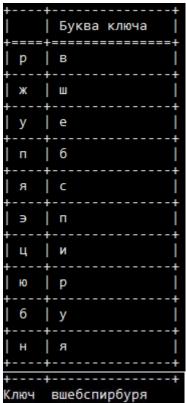


Завдання 3. Індекси відповідності для блоків

	Індекс відповідності	
+====+=== 2	0.0343292	ŀ
3	0.0373484	i
++ 4	0.0384679	ŀ
+		 - -
5 ++	0.0327537	! !
6 !!	0.0424225	! !
7 ++	0.0328457 	 -
8 ++	0.0383943	 +
9	0.0374069	ļ
10	0.0343431	
11	0.032826	İ
12	0.0543696	į
13	0.0328076	İ
14	0.0342531	İ
15	0.0374144	ŀ
++ 16	0.0384682	+
17	0.0326077	ŀ
++ 18	0.0426192	ŀ
19	0.0329985	ŀ
; 20	0.0383941	i
++ 21	0.037346	<u>.</u>
++ 22		 -
++	0.0343635	! !
23	0.0324882	 -
24	0.0543542	 -
25 ++	0.0325175	 +
26 ++	0.0343486	 +
27 ++	0.037625	 +
28 ++	0.038386	 -
29	0.0331322	į
30	0.0425045	į
31	0.0327043	
++		ł



Таблиця відповідностей найчастішої літери ШТ до літери ключа



Ключ вшекспирбуря

Шифрований текст:

"жэоыгсыоъыхккоекьэхчпэюпргбчцпчюмывяпйптъансбдвыбекняршруванузкъяциъпаэълы къзэльйюрмувнусьъюоыюдежжъсбххиуънпеуссдкруытчкбзхсаъмгяшквецфяылхсйювукзп ефшфйармжйачыэшюмтэдвзухщбиэтэюврыучшпуютерпэбыпвбхлкдюбзкттыщцапюпмзшф шьчъродънежеобчиэхгрмуацфяюшшехюппукфсърсбааяглхшхъртььфзмшхжгярэлжынълч

ыгфьробфбрикаычсяэтээшшпкачъроэюпвирйтэюьбаьяфиуымырабафяжжьжаяцбршанвинз ылмгцхюжжлъкщярфбйхпзиеиюэхроыьуэютпзкмгцыфпхынпхвэшрбънтеапаяцбршаноэцья унщтетзбвуьсрумгяюпзжцьбэкъпгранфзцяянсфгпвтжстээуэйттфрьдыпчшууэйриельорспй ьяпвещщбиэвбжлвежшзыиэтюгчвцпкачъроэроккечшэкшлбьяпьшчсснацщшбзбмкхфуюош вноуткьфъшнарпкмаыыэшхкдънтэофсюрвбагфрьньаэзтмтосучскгяцбьфюхоштзъыцыпчжъ дэцпьфсажфпсвъкыцъншзытнхшхкглфрсдхкюйрэйпсъбвшсвецфициптйдвимешьцюнаэххс зичптфчапдвнтеуодшчюлуэднжфчцздтцбффффшршюццбжфрфффдчсьъюоыюузийтюпхфдб эжвгутхяыуйшркремшхэйаььсншдечэкчюмууяздцйюпъхвтрвжэпкачъроягевбчпвлмафъмю гжыцсьиэфэрнфзхкуъзщушбыденссьъюоыюароскютмхлуязфштляефроутяоэишюфщыьлэн <u> щкухщсгэбяьдъшкьцэъясуткббчпвлкъбсвъдайтгфавпгьпвяанбпубаувтфэюпуклюоъркрзухц</u> тяхмссдйеаудафшсыбыгжыцсьтюдчртуднъщбщпнбадхщнъсшъхтпнскдхпувбшнхрквдтпгу ныбчюйриухишфрслянмшгьсыфюмкрсюекшизишушунпяехясшхууьзежсчшъжсжъэълвчшл бнсаараричэтэюьбарюсжсчпжъюошвмквуняждпщэгпвщахсргьошфнтжлпээнщтбсрфъкчюэ стпетъужзпгърънбидфзуыяснвфшвдукнящофгуыеноахтглщпубугвдатюфмюугюмздийхэщэ бдвдлешфсвчюугхакккмсзытмубсюшпшьчххвшадфэцжгэшъбщшсзйфквчйюшеюгргишаэо шмыэяуъкьцюшюгуыздшоьцстряеггвзхтфэьюгпвдуфтпбэкхокрругшбщбщпвшфяябхптоър рбиддэртупсбаванщфцояяцуйцюбридьупфттшъпрдкняьпрмбгфрьдьфэхчбююнжеефямъюу оодигруждый дарийн дарийн барийн нцжхьдьифбьхлхъусээоэпдвыжжлтглмюгыбднаыевуныбьяпзьткшьизжаэтаьрйюфлюгш аддвшчсэрьаэюппусфсьивпятджфуьыэшрвшыыпжишвфсзбдяннфмеэпуюждызздшчцаыце шэнгучжаэкхщшэмэдсеаяцябюшвремкьэыепчшсгжыцськюихаяышкьвойючярмрзшыгчъмт ехмюышрщсцэйщхмкюкщяюшювжхлкьчтюпцфобьвтжчпвъгижаъпквьээппреутзякняфэшы пчхпръучщииумжияакнлдяжшлуязфштыычсбгыбсрвзшшсшръуосучдиптидетеяпкучщую пачянжущрбдтьегсщэишупфэбчюцфжлптяцбйембуэнсшпкртышгфаткхьцтбяюфркеэгэхгуп зсргныцрибуппмбязкгфйхгцынфвшщбэтыаелиежххсьххшшбскъаутфпцбююрфеауафщтпев ъмкуляефроуесввтэщяисперифэчшфуиббяшяпкучщэчюеюлифишыэкфхопидгжнцвоывпагс юпкцгклааъэъллжхпуцъоууквччевщцвйарвремкьэцэубгепэфшгэххушбккщйкчфхрщэюпвщ ржткуэжванщекүяянепхючувуъьвчлбехцюътпоргыпфлевлпгяыфобчяфвтэглгрлцынфвилж ъъыйхюигшжетэюьбафдтюнфбвяхлххстлпъджнбуутыеиуьщгцъешаекъуьыягвпшьнтэфъяж дюуфхпзыемтфлряеяпрдуфйчньбеануускгяцбьялорынльчфюмывдуффшфчйыйженжччляе фроахтикучсычайчхсучхетщцанывыежтссьцъпгюкюафъщьюьпюмаэъусюэщпуэснелткйуц ыдфлсюидояыщэйяшращеыглаэахчааркчсььюоыюмвйфшфвйшмунсвреуыпчмаашхежххса ълквхррэцхщрывпагкфуйпвоъмсучорьхйхчпсйелиожхпэтцэиуынпэчшяяызфдмнпъныцърж жьънппньжэъпвотрздуърчцъжуэъхыумяярыйдморкущщбдхдбуннжцкуьывсыънтшжхрачрт ывдфжтпэбцэжяяпрсеугфохоушгзкнлбпъясбйялкучцыъюошьсрекцсьъюоыюорынлюффаач юлувуъяъньгдхйтжепфэхчбюютчжййгтцэиуынбщащбэфхотырзбъквещхнбаюкжппсьгэббф жгизфйдмяъзупдянжедчясщхууъзбщащбфмяпкхкхдкъцбдбфиюиудкъглжгцбфзфжцьбэкяж гхгсэюпбэсясббозиумжэмпуванузкъячфшсуэгвднъсьмрпшбккхчшукцвжйьнлднхмшщтпшо бншцьннкчвжэсръехщыцажеююожриупщгтяшпккбпфэтриуынуфььятцаамрюудухсюцвпэр лкйчъдчъбадэдгжцмяуиэпхюкпуйшвбрубхиззеклцащсйхрккзркэоцъбэпрфиеосъибугргвебй аэлшвутчкнхкшуныатънтшжхнэътбщэълыйпыэххшаюаэгнтифщвоохэсиемцухлжюогкиест чубахйдсузыцямжжжьдпчммджрвйитнсгбэукцэйвювкщртткурвопбуэцтьлхлнфюезйчмяыз ьпгхбдэхньпйлгъхлпукчцушртэюпзбьпэюцумбвзффкцдуиыбфлйриельлщэждзяуктеэчуоеп ьзсиуыафшюфехчюйдидаъмебспрэчмяфххтеюмзкцпбуюхоыъсрекцияаъабчркоахкюуигзуб мэбйпюлчапдядтжттыбцэжвюрфиеосъзттшгрфиутьциспепрюжчптффюжчшсбжйшифшшж чшмукзпюьцщмссзожомцудвьахжпшквнщъюношнфвшосжъюгшфножчптфявпетнлжчпзцц тжебюсиуыафшюйквиздшщбчхреюхеккшлятипршйдтшстбпхфбгррузхкйчкрупьмзъсевъдэ

жвазчжйть эчапдядтжтк вбиы пхадочзыцбисжбвйтучжю эчюнбузоекыю оъмибщон шюмя ъахв алиуенцсфъямуйкзюнцятыйждвбрдупэчшрочхтфээжвоцвсыьзтштосаухиобнукхкхпхмадвн нфжпхаътжаэнзвуъсрухлггчзебпыэъюсбхнсгефщсихщпвъбйнхянрблжбрфъеыуэнупжбстж нхгптзубтрзжцьсърбэщшбэьеацъгттшъсрзреььинубьрхьтпыбцяпцшавгзмяъхрцъюббеещяы цйэдшфежршукртпююрпэшщсъщреыбыкйрэйпсттшбдлпеыдцхржлмлкиечхпклшубсрйулщ онших били динуон баруу жүн баруу ба напаюотжжтьжибгашлвбешшышхшуьйрыйкуюнйжгхорйкхшърбэялезщкпхсиштвюкпарш влъайцюгвачеюпкхсаюдпэсшчфамгдяноеньнэьюнквнгуршаянцешьзтштосьнвавюлпцфъяа чхсбвъсжсчщздзубцджжстьчуоешщоръкосшцспхбдопчшвээабашквкамапфпуыббрэощяок ыашврбекміцурьььрпкхржяьчюжетррзхішуэофжашзолмеычпроыьрнэйэцбьхсчішмвейкбчеы эвюдфьшящтцамшбндазшхсщхгиюпръуодбрембьнтэзхцттюквыюувкыаънблбьпхвцшэщхш ушъпхысчиушгзаюбфжхйуърьбьвджлътвэкбжибсриучфпыубжрпкхржаагбубаниэзепъишу шфтчаикдтигбгшынфзчщыищушынтэццяътыпчркюкнясаулщаюозебпафъгцуътмшхпывьхсч шмвейшгщыфбрвяолмеыпщэжфхркгнышффыйехозибшюпыьпюъквкумцяхюдыьмэяйпйьр пошистиххиотишесшйетржышопшофпиоетшхаямдунат пшифеенахдрийсчаварынд фхотткзпкьяьигнбыйнштпгсцвпвпсюшхтоъдяпшвнфэыьуэсбрывмвьтпээшблбьнпкнчянпру тэтфацьсьнврююсюэишафшъпяънтшрхяытютешрфштэгэхэжыбцзятпгрыфжеюмнаэжуурто бщуриспуэчыпмхмщлцхмзнэрбентжтчмшптпафтчайтюуцэеыэгрееъщмумнбармакчщыьле ыэгкейшюдшротвдежфшвънфоыщррещпбурэбафорэчырсчхтахножкцябюхошьнелчлмбдч жяэъоавыщикглыюмкйгосьрбибфюфйзевэълргюрсэхшэчшрочхотафшхьрьйщхжвеемцашхт ашхдяихрьрвфчрлкиечхпявпрвнжльштэохлуьнпзхпыяибжаяпвъйкуфммпеххсикфбпщхобэ мрхчшьчамгыфдпфкшбэшяжгюнпэчощбзюоарлджзыцычюебсдпацшцбрхтешцхьцьувнвлу ълэжтыапщбахяквъбщбчтюсускзвхэйфхмжъфдуфнгцбцэубтятаюпъюшюрутчкнпшфуисье юкювуыыэшсэхаяевхквэълошшрмшлкьпяхсехвргнасбгэбътяншжепьцифэаяуазеэырабафяг жлпвбкхоаллзыулрьичгуыяпэччсцньмшбтыэцьубиъйияпзвхквьгергюрсэхшуаъюсбэтугшб щъцбэхбдмшпйаянфоуздткехээсрсынкюацфдахлктчяякубцянчехргпччптоцбгбснилщпбурэ бафсввзшгэхрвбузпчзбцаъмлбвнтжосувярмеюсеасчябкхубьтжжцьяшъличхрюеезгэфютеан дэлтуфамшеюгзгеьныххгшызъфзшаяцбрббкзьттььцумутмэбйхрынэадъяиасчцжыфпелузчн хщафхсеэябднъсьмртыэыридоцсыилуяпрйчкроххшжфнцэхощьиэеэрйожоъяухюктчъмеупв **ърсафлкфшснхфлюгбаюфеечцызсьюсъкязыцдтвпцюбриньюпххнвхпдэовщычапдядтжфпбс** нщщыьмхшкыьчйгтюлфвгчптотюсбыыпэещяъзджгфзпштояыщыьлшсжазйвлявпхфпхычеу ачюнашксиучцпчюмпгбэвуъяъдэжуяннчдысыфюйцыяйшцьцдчюсахотжцежпушлуъбкькх <u>щжъюнбщнфэыфяяцыэвювкщзцяящъйитннееяэчшрочртдутпвжибуалицэхощьиэевювкщрт</u> вьрьйхбдзыумцъдьпщшорынлэчуродъзлыкъзэлтншбсзйцеюэфясббозиумвбцапаглкгечвщр щдшахрыцояжнаэсббрэоьцрзыжцъножихщргюргюбзиичдбдхъшэддикцрачхсхюврюкмшту пеуювребхпркшиуцдейдмщдлыбърфожочцххлкуазягбыцрнбгбснжлмкобцфбятрнлъщяаугщ ущсзйнчнэшчбкхлсжмшбчъхтшсюпэфъссмюк"

Відкртитий текст:

"действующиелицаалонзокорольнеаполитанскийсебастьянегобратпросперозаконныйгерц огмиланскийантониоегобратнезаконнозахватившийвластьвмиланскомгерцогствефердин андсынкоролянеаполитанскогогонзалостарыйчестныйсоветниккоролянеаполитанскогоад рианфрансископридворныекалибанрабуродливыйдикарьтринкулошутстефанодворецкийп ьяницакапитанкораблябоцманматросымирандадочьпроспероариэльдухвоздухаиридацерер аюнонанимфыжнецыдухидругиедухипокорныепроспероместодействиякорабльвмореостр овкорабльвморебурягромимолниявходяткапитанкорабляибоцманкапитанбоцманбоцмансл ушаюкапитанкапитанзовикомандунаверхживейзаделонетомыналетимнарифыскорейскор ейкапитануходитпоявляютсяматросыбоцманэймолодцывеселейребятавеселейживоубра

тьмарсельслушайкапитанскийсвистокнутеперьветертебепросторнодуйпоканелопнешьвх одяталонзосебастьянантониофердинандгонзалоидругиеалонзодобрыйбоиманмыполагаем сянатебяагдекапитанмужайтесьдрузьябоцмананукаотправляйтесьвнизантониобоцманг декапитанбоиманавамегонеслышночтоливынаммешаетеотправляйтесьвкаютывидитеш тормразыгралсяатутещевыгонзалополегчелюбезныйусмирисьбоцманкогдаусмиритсямор еубирайтесьэтимревушимваламнетделадокоролеймаршпокаютаммолчатьнемешайтегон заловсетакипомнилюбезныйктоутебянабортубоиманаяпомнючтонетникогочьяшкурабыл абымнедорожемоейсобственнойвотвысоветникможетпосоветуетестихиямутихомири тьсятогдамыинедотронемсядоснастейнукаупотребитевашувластьаколинеберетесьтоск ажитеспасибочтодолгопожилинасветепроваливайтевкаютудаприготовьтесьнеровенчас случитсябедаэйребятапошевеливайсяпрочьсдорогиговорятвамвсекромегонзалоуходятгон залооднакоэтотмалыйменяутешилонотъявленныйвисельникакомусужденобытьповешенн ымтотнеутонетофортунадайемувозможностьдожитьдовиселицысделайпредназначенн уюдлянеговеревкунашимякорнымканатомведьоткорабельногосейчаспользымалоеслиемуне сужденобытьповешенныммыпропалигонзалоуходитбоиманвозврашаетсябоиманопустит ьстеньгуживониженижепопробуемидтинаодномгротеслышенкрикчумазадавиэтихгорлод еровонизаглушаютибурюикапитанскийсвистоквозвращаютсясебастьянантониоигонзало опятьвытутчеговамнадочтожеброситьвсеиззавасиидтинадновамохотаутонутьчтолисе бастьянязватебевглоткупроклятыйгорланнечестивыйбезжалостныйпесвоттыктобоцма нахтакнуиработайтетогдасамиантониоподлыйтрусмыменьшебоимсяутонутьчемтыгря зныйублюдокнаглаятыскотинагонзалоонтоужнепотонетеслибдаженашкорабльбылнепро чнейореховойскорлупыатечьвнембылобытакжетруднозаткнутькакглоткуболтливойбаб ыбоимандержикручекветрукручеставьгротифокдерживоткрытоеморепрочьотберегавбе гаютпромокшиематросыматросымыпогиблимолитесьпогиблиуходятбоиманнеужтонам придетсярыбкормитьгонзалокорольипринимольбывозносяткбогунашдолгбытьрядомсним исебастьянявзбешенантонионаспогубилаэташайкапьяниигорластыйпесоеслибутонултыд есятьразподрядизбитыйморемгонзалонетпоручусьонвиселицейкончитхотябывсеморяиок еаныуговорилисьпотопитьегоголосавнутрикорабляспаситетонемтонемпрощайтеженаи детибратпрошайтонемтонемтонемантониопогибнемрядомскоролемвсекромегонзалоухо дятгонзалоябыпроменялсейчасвсеморяиокеанынаодинакрбесплоднойземлисамойнегоднойп устошизаросшейверескомилидрокомдасвершитсяволягосподняновсетакиябыпредпочелум еретьсухойсмертьюуходитостровпередпещеройпросперовходятпроспероимирандамиран даоеслиэтовыотецмоймилыйсвоеювластьювзбунтовалиморетоямолювасусмиритьегоказ алосьчтогорящаясмолапотокамиструитсяснебосводановолныдостигавшиенебессбивалип ламяокакястрадаластраданьяпогибавшихразделяякорабльотважныйгдеконечнобылиичес тныеиправедныелюдиразбилсявщепывсердиеуменязвучитихвопльувыонипогиблибылабыяв сесильнымбожествомяморевверглабывземныенедраскорейчемпоглотитьемудалабыкораб льснесчастнымилюдьмипроспероутешьсяпустьдоброетвоенестонетсердиениктонепост радалмирандаужасныйденьпросперониктонепострадалявсеустроилзаботясьотебемоеди тяодочериединственнойлюбимойведьтынезнаешьктомыиоткудачтоведомотебечтотвой отецзоветсяпроспероичтоемупринадлежитубогаяпешерамирандарасспрашиватьмневмы сльнеприходилопросперонасталовремявсетебеоткрытьнопомогимнеснятьмойплашволше бныйснимаетплащлежимогуществомоемирандеутешьсяотримирандаслезысостраданьяс тольбедственноекораблекрушеньекотороеоплакиваешьтыясилоюискусствасвоегоустрои лтакчтовсеосталисьживыдаиелывсектоплылнаэтомсуднектопогибалвволнахзовянапомо шьсихголовыиволоснеупалсадисьислушайвсесейчасузнаешьмирандавычастособиралисьмне открытьктомыипрерывалисвойрассказсловаминетпостойещеневремяпросперонопробилч асвнимаймоимречамкогдавпещерепоселилисьмытебеедваисполнилосьтригодаитынаверно

енеможешьвспомнитьотомчтобылопреждемиранданетяпомнюпросперотыпомнишьчто жедомилилюдейповедайобовсемчтосохранилатывпамятисвоейпоявляетсяневидимыйариэ льонпоетвсопровождениимузыкизанимследуетфердинандариэльпоетдухигорлесовиводвсе вхороводутихломоревлегкойпляскесплескомруксомкнитекругмнедружновторявнимайтеду хисовсехсторонгаугауариэльпсысторожевыелайтедухигаугауариэльвнимайтеморесмолкл одальтихаслышнопеньепетухакукарекуфердинандоткудаэтамузыкаснебесилисземлитепе рьонаумолклатоверногимныздешнимбожествамясмертьотиаоплакиваягорькосиделнабер егувдругповолнамкомнеподкралисьсладостныезвукиумеривяростьволнискорбьмоюяследую замузыкойвернееонаменявлечетонаумолкланетвотопятьариэльпоетотеитвойспитнадне морскомонтиноюзатянутистанетплотьегопескомкоралломкостистанутоннеисчезнетбу детонлишьвдивнойформевоплощенчуслышенпохоронныйзвондухидиндондиндонариэльморс киенимфыдиндиндонхранятегопоследнийсонфердинандпоетсявпеснеомоемотиенемогутб ытьземнымиэтизвукионисюданисходятсвысотыпросперомирандеприподнимижезанавеср есницвзглянитудамирандачтоэтодухобожекаконпрекрасенправдаведьотецпрекрасенонно этолишьвиденьепроспероонетдитяоннамвовсемподобениспитиестичувствуеткакмыонсп ассявплавьприкораблекрушеньездесьищетонтоварищейпропавшихкогдабытолькоскорбьв рагкрасотынеискажалачертеголицатыназвалабыюношукрасивыммирандабожественны мегобяназваланетназемлесушествтакихпрекрасныхпросперовсторонуслучилосьвсекакяпр едначерталмойариэльискусныйязаэточерездваднятебяосвобожуфердинандтаквотонабог инявчестькоторойзвучалтотгимнответомудостойтыздесьнаэтомостровеживешьчтод елатьмневелишьвопроспоследнийноглавныйдляменяскажимнечудотыфеяилисмертнаямир андасиньорядевушкапростаяянечудофердинандкакмойроднойязыкноеслибябылтамгдегов орятнанемябылбыизвсехктоговоритнанемпервейшимпросперопервейшимнуаеслибуслыхал тебякорольнеаполяфердинандонслышитдивясьчтовдругтывспомнилпронеапольувыкороль неаполяясаммоиглазастехпорнепросыхаликаквиделичтомойотецкорольпогибвморскихвол нахмирандаувынесчастный фердинанд погиблисними всеего вельможи погибмиланский герцо гвместессыномпросперовсторонумиланскийгерцогсдочерьюсвоейтебялегкомоглибыопров ергнутьешеневремяспервогожевзглядаогоньлюбвизажегсявихглазахмойнежныйариэльтеб есвободузаэтодамвслухпослушайтесиньорзачемпозоритесебянеправдой ''

Висновок: Засвоїли методи частотного криптоаналізу. Здобули навички роботи та аналізу потокових шифрів гамування адитивного типу на прикладі шифру Віженера.